IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
COLUMBUS DIVISION

ELEANOR GRIFFIN, *individually and on behalf of all others similarly situated,* Plaintiff, v. AFLAC INCORPORATED, Defendant.	Case No.: 4:25-cv-00183 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Eleanor Griffin ("Plaintiff") brings this Class Action Complaint on behalf of herself, and all others similarly situated, against Defendant Aflac Incorporated ("Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which is based on personal knowledge:

NATURE OF THE ACTION

1. This class action arises out of Defendant's failure to implement reasonable and industry standard data security practices to properly secure, safeguard, and adequately destroy Plaintiff and Class Members' sensitive personal information that it had acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack to compromise sensitive information entrusted to Defendant (the "Data Breach") that,

upon information and belief, contained personally identifiable information ("PII[1]" or "Private Information") and protected health information ("PHI", and collectively with "PII", "Private Information") of Plaintiff and other individuals ("the Class"), that was compromised in a cyber incident (the "Data Breach") in June 2025.

3. Defendant is a Fortune 500 company that provides financial protection to millions of policyholders and customers through its subsidiaries in the U.S. and Japan.

4. On June 12, 2025, Defendant identified suspicious activity on its IT Network.[2] In response, Defendant promptly initiated its cyber incident response protocol and launched an investigation to determine the nature and scope of the Data Breach.[3]

5. Defendant has confirmed that the Data Breach was led by a sophisticated cybercrime group.[4]

6. On or about April 2, 2024, Defendant discovered that an unauthorized actor or actors accessed and acquired files from its IT systems on or about April 1,

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).
[2] *Exhibit 1*, Plaintiff's Notice Email.
[3] *Id.*
[4] *Id.*

2024.[5] In response, Defendant launched an investigation to determine the nature and scope of the Data Breach.[6]

7. Upon information and belief, Defendant's investigation determined that the following types of Private Information were compromised because of the Data Breach: health information, Social Security numbers, and/or other personal information, related to customers, beneficiaries, employees, agents, and other individuals in its U.S. business.[7]

8. Recently, Defendant began sending out notice emails to customers informing them about the Data Breach.[8]

9. The Data Breach was a direct result of Defendant's failure to adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information which it was hired to protect.

10. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*

11. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; and (6) failing to encrypt or adequately encrypt the Private Information.

12. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to protect Plaintiff and Class Members Private Information from unauthorized intrusions; failing to disclose that it did not have adequately robust security practices to safeguard Plaintiff and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

13. Plaintiff and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

14. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

15. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the Dark Web.

16. Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

17. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs

incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of their Private Information; and (f) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

18. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself, and all similarly situated individuals whose Private Information was accessed during the Data Breach.

19. Accordingly, Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

20. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

21. Plaintiff Eleanor Griffin, at all times relevant hereto, was a citizen and resident of Calumet City, Illinois.

22. Defendant is a corporation organized under the laws of the State of Georgia, maintaining its principal place of business at 1932 Wynnton Rd, Columbus, Georgia, 31999.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of Class Members exceeds 100, some of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and maintained Plaintiff and Class Members Private Information in this District.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District and maintains Plaintiff's and Class Members' Private Information in this District.

FACTUAL BACKGROUND

A. Defendant's Business

26. Defendant is a Fortune 500 company that provides financial protection to millions of policyholders and customers through its subsidiaries in the U.S. and Japan.

27. Upon information and belief, in the course of collecting Private Information from individuals', including Plaintiff and Class Members, Defendant promised to provide confidentiality and adequate security for the data it collected from individuals' through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

28. At all relevant times, Defendant knew it maintained sensitive Private Information and that, as a result, Private Information is a sensitive target for cybercriminals.

29. Defendant obtained Plaintiff and Class Members Private Information with reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. Despite its alleged commitments to securing sensitive data, Defendant did not follow industry standard practices in individuals' Private Information and

failed to protect the Private Information of Plaintiff and the proposed Class members from unauthorized disclosure in the Data Breach.

B. The Data Breach

31. On June 12, 2025, Defendant identified suspicious activity on its IT Network.[9] In response, Defendant promptly initiated its cyber incident response protocol and launched an investigation to determine the nature and scope of the Data Breach.[10]

32. Defendant has confirmed that the Data Breach was led by a sophisticated cybercrime group.[11]

33. On or about April 2, 2024, Defendant discovered that an unauthorized actor or actors accessed and acquired files from its IT systems on or about April 1, 2024.[12] In response, Defendant launched an investigation to determine the nature and scope of the Data Breach.[13]

34. Upon information and belief, Defendant's investigation determined that the following types of Private Information were compromised because of the Data Breach: health information, Social Security numbers, and/or other personal

[9] *Exhibit 1*, Plaintiff's Notice Email.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*

information, related to customers, beneficiaries, employees, agents, and other individuals in its U.S. business.[14]

35. Recently, Defendant began sending out notice emails to customers informing them about the Data Breach.[15]

36. Plaintiff's claims arise from Defendant's failure to safeguard his Private Information and failure to provide timely notice of the Data Breach.

37. Defendant failed to take precautions designed to keep individuals' Private Information secure.

38. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

39. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

40. Defendant failed to take adequate measures to protect Plaintiff and Class Members Private Information against unauthorized access.

[14] *Id.*
[15] *Id.*

41. The Private Information that was exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

42. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[16] Defendant failed to disclose that its security practices were inadequate to reasonably safeguard individuals' sensitive Private Information.

43. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[17] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

D. The Harm Caused by the Data Breach Now and Going Forward

44. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[18]

45. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft. Plaintiff and Class Members face a substantial risk of identity theft.

46. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search

[16] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited June 20, 2025).
[17] *Id.*
[18] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited June 20, 2025).

engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

47. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[19]

48. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[20] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[21] As data breaches continue to reveal, "PII about employees, clients and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[22]

49. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[23]

50. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of

[19] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 20, 2025).
[20] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited June 20, 2025).
[21] *Id.*
[22] *Id.*
[23] *Id.*

complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[24]

51. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[25] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant notified impacted people more than a year after learning of the Data Breach.

52. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further

[24] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited June 20, 2025).

[25] *Id.*

injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

53. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

54. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that individuals' Private Information were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

55. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

E. Plaintiff Eleanor Griffin's Experience

56. Plaintiff Griffin is a customer of Defendant.

57. Plaintiff provided Defendant with her Private Information as a condition of receiving services from Defendant.

58. On June 20, 2025, Defendant sent Plaintiff a notice email informing her about the Data Breach.

59. Defendant was in possession of Plaintiff's Private Information before, during and after the Data Breach.

60. Plaintiff reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

61. Plaintiff greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

62. Plaintiff stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

63. As a result of the Data Breach, Plaintiff has spent time researching the Data Breach, reviewing her bank accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

64. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress that her Private Information was acquired by criminals as a result of the Data Breach.

65. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

66. Plaintiff has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

67. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has been stolen and likely published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that Defendant obtained from Plaintiff; and (g) other economic and non-economic harm.

CLASS ALLEGATIONS

68. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose Private Information was compromised in the Defendant's Data Breach disclosed in June 2025.

69. Excluded from the Class are Defendant, its subsidiaries and affiliates, its officers, directors and members of its immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of its immediate families.

70. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

71. **Numerosity**. The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

72. **Commonality**. This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' Private Information;

c. Whether Defendant breached its obligations to maintain Plaintiff and the Class Members' medical information in confidence;

d. Whether Defendant was negligent in collecting, storing and safeguarding Plaintiff and Class Members' Private Information, and breached its duties thereby;

e. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

f. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and

g. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

73. **Typicality**. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant safeguard Private Information. Plaintiff and Class Members' information was stored by Defendant's software, each having their Private Information obtained by an unauthorized third party.

74. **Adequacy of Representation**. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class

Members she seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

75. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its common law and statutory duties to secure Private Information, then Plaintiff and each Class Member suffered damages from the exposure of sensitive Private Information in the Data Breach.

76. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

77. **Manageability.** The precise size of the Class is unknown without the disclosure of Defendant's records. The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and

adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

78. Plaintiff restates and realleges paragraphs 1 through 77 above as if fully set forth herein.

79. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information and to keep it from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

80. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

81. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

82. Defendant breached its duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things:

(a) mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; and (f) failing to follow their its policies and practices published on its own website.

83. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, the Private Information would not have been compromised.

84. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

85. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with the

industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of a data breach involving the Private Information of their customers.

86. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

87. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

88. The harm that has occurred because of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

89. Defendant violated its own policies by actively disclosing Plaintiff and Class Members' Private Information; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information; failing to maintain the confidentiality of Plaintiff and Class Members' records; and by failing to provide timely notice of the breach of Private Information to Plaintiff and Class Members.

90. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant ould safeguard Plaintiff and Class

Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' data;

i. Loss of their privacy and confidentiality in their Private Information;

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

91. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

92. Plaintiff restates and realleges paragraphs 1 to 77 above as if fully set forth herein.

93. When Plaintiff and Class Members provided their Private Information to Defendant, Plaintiff and Class Members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such

information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

94. Plaintiff and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant.

95. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

96. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the Private Information of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach. As noted *supra*, Defendant waited more than a year after the Data Breach occurred, to notify impacted individuals' that their Private Information was compromised.

97. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

98. Plaintiff restates and realleges paragraphs 1 to 77 as if fully set forth herein.

99. Plaintiff brings this claim in the alternative to her breach of implied contract claim above.

100. Plaintiff and Class Members conferred a benefit on Defendant by way of providing Defendant with their Private Information, in exchange for obtaining services from Defendant.

101. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members.

102. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and Class Members Private Information because Defendant failed to provide adequate safeguards and security measures to protect Plaintiff and Class Members' Private Information.

103. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

104. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

105. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a

periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying

information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss

of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June 20, 2025

Respectfully,

By. */s/ Casondra Turner*

Casondra Turner (GA Bar No. 418426)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929

Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Counsel for Plaintiff and the Proposed Class